



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,434	12/10/2003	Christoph Gouguenheim	200207237-1	2133
22879 7590 12/19/2007 HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400			EXAMINER LASHLEY, LAUREL L	
			ART UNIT 2132	PAPER NUMBER
			NOTIFICATION DATE 12/19/2007	DELIVERY MODE ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM  
mkraft@hp.com  
ipa.mail@hp.com

## Office Action Summary

Application No.

10/733,434

Applicant(s)

GOUGUENHEIM ET AL.

Examiner

Laurel Lashley

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 03 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-28 and 30-36 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-28 and 30-36 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 03 October 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Response to Amendment***

1. The Applicant's amendments to the claims and specification filed 10/03/2007 have been accepted and entered. Claim 29 has been cancelled, therefore claims 1 – 28 and 30- 36 are still pending.

### ***Drawings***

2. The drawings were received on 10/03/2007. These drawings are acceptable.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1 – 36 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Independent Claims 1 and 36 recite the limitation "the first key", "the insecure device", and "the second key". There is insufficient antecedent basis for these limitations in the claims. Claims dependent on claim 1 also recite one or all of the above limitations and are therefore rejected too.

Independent Claims 11, 19 and 28 recites the limitation "the first key", and "the second key". There is insufficient antecedent basis for these limitations in the claims. Claims dependent on claims 11, 19 and 28 also recite one or all of the above limitations and are therefore rejected too.

Independent Claim 17 recites the limitation "the first key" and "the identifier". There is insufficient antecedent basis for these limitations in the claim. Claims dependent on claim 17 also recite one or all of the above limitations and are therefore rejected too.

Independent Claim 26 recites the limitation "the insecure device". There is insufficient antecedent basis for this limitation in the claim.

Claim 30 recites the limitation "the secure device". There is insufficient antecedent basis for this limitation in the claim.

This rejection is maintained as in the non-final Office action mailed 07/03/07 because the claim language fails to contain any earlier recitation of the terms used. Appropriate correction is required.

### ***Response to Arguments***

3. Applicant's arguments filed 10/03/2007 have been fully considered but they are not persuasive. It is Applicant's argument that Kocher fail to teach creating a second key from a first key and a message unique to an insecure device. The Examiner respectfully disagrees. Kocher discloses that the key derivation message (KDM) is generated and transmitted with corresponding digital content. Since digital content is variable, it is inherent that the message is unique to the device since the digital content being transmitted is unique to the device. (see column 8, lines 17 – 28)

4. The Applicant further contends that Kocher fails to teach the hash function, the message unique to the insecure device, or using the hash function to create a second key from the first key and the message unique to the insecure device. Again, the Examiner respectfully disagrees. Kocher discloses a pseudoassymmetric function (see column 8, lines 28 – 31) which prohibits inverse computation, therefore maintaining the security of encrypted content. Furthermore Kocher discloses that the content distribution key (i.e. the second key) is generated by using the rights key hashed with the key derivation message (see column 10, lines 42-51; column 11, lines 33 – 42, 59 - 61).

5. The Applicant asserts that Kocher fails to teach the content provider receiving a unique identifier for the playback device from the playback device. Kocher discloses that the playback device transfers the KDM to the cryptographic rights unit (CRU) which operates collaboratively with the content provider to distribute digital content (see column 9, lines 16 – 28).

6. The Applicant argues that Kocher fails to teach the smart card is used to sell a file, and fails to teach creating a third key for the peer and sending the third key to both the peer and the playback device. The Examiner respectfully disagrees. Kocher discloses a device key, specific to a device, employing security related parameters (e.g. smartcard) used in electronic transaction for distribution of digital content (see column 7, lines 65 – 67: device key; column 9, lines 1 – 6)

For at least these reasons the Examiner maintains the rejection below:

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1 – 28 and 30- 36 are rejected under 35 U.S.C. 102(b) as being anticipated by Kocher et al. in US Patent No. 6289455 (hereinafter US '455).

8. For claim 1 and similar claims 11, 17, 19, 26, 28 and 36, US '455 discloses:

A secure token (see column 8, lines 12 – 16) for use with an encrypted file (see column 8, lines 1 – 7) and an insecure decryption device (see column 8, lines 22 – 28), the secure token comprising a processor for protecting a first cryptographic key against unauthorized access (see column 8, lines 52 – 55), and creating a second cryptographic key (see column 7, lines 46 – 47) from the first key and a message unique (see column 8, lines 17- 28) to the insecure device,

the second key usable for file decryption by the insecure device. (see Abstract: rights key used to authorized usage; column 9, lines 42 – 52: content decryption key comprising and key derivation message and rights key used to decrypt digital content; column 11, lines 33 – 65 : accessing content)

For claim 2 and similar claims 30 and 31, US '455 discloses:

The secure token of claim 1, wherein the secure token includes a smart card, the smart card including the processor. (see column 8, lines 12 – 16)

For claim 3 and similar claim 20, US '455 discloses:

The secure token of claim 1, wherein the processor uses a hash function to create the second key from the message and the first key. (see column 8, lines 52 – 55: rights key required...; column 11, lines 59 - 60: hash function)

For claim 4 and similar claims 12, 18, 21, and 33 US '455 discloses:

The secure token of claim 1, wherein the secure token performs an electronic transaction to obtain the first key. (see column 8, lines 45 – 50)

For claim 5 and similar claims 13 and 22, US '455 discloses:

The secure token of claim 4, wherein the secure token conducts a transaction with a server to purchase a desired file; and wherein the secure token receives the first key from the server (see column 9, lines 1 – 6; column 10, lines 50 – 55).

For claim 6 and similar claims 14 and 23, US '455 discloses:

The secure token of claim 4, wherein the secure token conducts a transaction with a peer to purchase a file; and wherein the secure token receives the first key from the peer (see column 9, lines 1 – 6; column 10, lines 50 – 55).

For claim 7 and similar claims 15 and 24, US '455 discloses:

The secure token of claim 4, wherein the secure token conducts a transaction with a peer to sell

a file; and wherein the secure token sends the first key to the peer (see column 7, lines 65 – 67: device key; column 9, lines 1 - 6).

For claim 8 and similar claims 16 and 25, US '455 discloses:

The secure token of claim 7, wherein the secure token creates a third key that is unique to the peer, and sends the third key to the insecure device and the peer (see column 7, lines 65 – 67: device key; column 9, lines 1 – 6).

For claim 9 and similar claim 27, US '455 discloses:

The secure token of claim 1, further comprising means for receiving the first key and encrypted data (see column 22, lines 35 – 40), wherein the insecure device uses the second key to decrypt the encrypted data (see column 9, lines 42 – 52: playback decrypts content with content decryption key).

For claim 10 and similar claim 34, US '455 discloses:

The secure token of claim 1, wherein processing power of the secure token is significantly less than processing power of the insecure device. (see column 4, lines 23 – 27)

For claim 35, US '455 discloses:

The system of claim 28, further comprising a peer-to-peer application for identifying peers having desired files. (see column 9, lines 7 – 15)

### ***Conclusion***

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

10. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

Application/Control Number:  
10/733,434  
Art Unit: 2132

Page 7

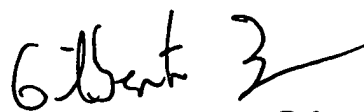
will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley  
Examiner  
Art Unit 2132  
13 December 2007  
LL

  
GILBERTO BARRON JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100